SecurityExpressions™ Audit and Compliance Server 4.x

Getting Started Guide

altiris

Notice

SecurityExpressions Audit and Compliance Server 4.0 Getting Started Guide

Document Date: February 28, 2007

Contents

Information Resources

This preface contains the following information to help you get started:

Online Documentation

We provide software documentation in the following electronic formats: online Help; Adobe® Acrobat® .pdf files; and Release Notes (.htm).

Online Help

Comprehensive help is available from the **Help** menu. To access context-sensitive Help, click the Help icon on the Web page.

PDF Files

The SecurityExpressions Server software includes a user guide in .pdf format in the installation Zip file. You must have Acrobat® Reader installed to read the files.

Installing Acrobat Reader

If you do not have a copy of Acrobat Reader, you can download a free copy from the Adobe Web site at www.adobe.com.

Using PDF Files

With .pdf files, you can navigate through a document quickly and perform full-text searches. You can also view the .pdf files online, distribute them to multiple users electronically, or print them. Double-click .pdf files to open them, and then move through the document by clicking topic headings in the left pane or blue hypertext links in the text. To print copies, choose **Print** from the **File** menu.

Formatting Conventions

The following formatting conventions are observed throughout this guide:

- **Bold** text designates user interface information appearing in the documentation.
- *Italic* text emphasizes words and book titles.
- `Courier` text shows literal text as you would enter it, or as it would appear on screen.
- `<variables>` are enclosed in less than (<) and greater than (>) symbols, and are often placed in `Courier` formatted text.
- Title caps (initial letter of words capitalized) are used in major headings and dialog box titles.
- Blue hypertext links you to another part of the document.

Contacting Us

Altiris, Inc. is a pioneer of IT lifecycle management software that allows IT organizations to easily manage, secure and service desktops, notebooks, thin clients, handhelds, industry-standard servers, and heterogeneous software including Windows, Linux, and UNIX. Altiris automates and simplifies IT projects throughout the life of an asset to reduce the cost and complexity of management.

Corporate Headquarters and Sales

588 W. 400 S.

Lindon, UT 84042 USA

http://www.altiris.com

Toll Free: +1 888 252 5551

Outside the US: +1 801 226 8500

Fax: +1 801 226 1812

Ask to speak to a sales representative about any sales issues, including the latest products, training, upgrade options, prices, and your software purchase.

E-mail: security-sales@altiris.com

If you have a technical question, however, please contact customer support.

Support and Maintenance

Annual support contracts include e-mail and telephone support. Annual Upgrade Protection, or AUP, allows registered software users to upgrade to any version of the registered product that is released during the coverage period without paying an upgrade charge and includes a subscription to the Policy File Library. This service is distinct from, and designed to work in conjunction with, customer support to give you the best possible experience with our products.

Pricing and additional information about support and maintenance is available at http://www.altiris.com/support.

Customer Support

We provide e-mail and telephone support to those who purchased a support plan. Before you contact customer support, please collect the following information:

The version number of the software.

The operating system on the computer running the software. Include the number of the last service pack installed, if applicable.

The name and version number of the relational database you use with the software.

The name and version number of the SIF file or SPF file involved, if applicable.

The software's license key.

A brief description of the problem with steps on how to reproduce it.

Error messages you received, if any.

E-mail: support@altiris.com

Phone: +1 801 225 8500

CHAPTER 1

Introduction to SecurityExpressions Audit & Compliance Server

The SecurityExpressions product family consists of the SecurityExpressions Console and the SecurityExpressions Audit & Compliance Server. The SecurityExpressions Console allows you to audit interactively, schedule audits, create notifications, report, and remediate from a stand-alone desktop application that integrates with a central database. The SecurityExpressions Audit & Compliance Server performs many similar functions on a server managed through a Web browser.

SecurityExpressions Overview

The SecurityExpressions Audit & Compliance Server performs audits and reports audit results. When using the SecurityExpressions Audit & Compliance Server, you may also use the SecurityExpressions Console for customizing policy files, managing stored credentials, and advanced reporting. The SecurityExpressions Console and SecurityExpressions Audit & Compliance Server can share a database so that each works with and reports on a consistent set of Machine Lists, credentials, and audit data.

SecurityExpressions automates the process of deploying, assessing and maintaining consistent security policies on networks of devices running Microsoft Windows and UNIX operating systems. It helps organizations with security management and large-scale systems hardening. Enterprises can perform security audits on scheduled intervals or upon certain criteria such as a system connecting to a network, that you can set depending on the value of your data and risk tolerance.

It is very difficult for one person or department to keep track of the ever-changing data security environment. IT people often work in a reactive mode. A computer and information security audit can be an extremely difficult undertaking. The growing complexity of information systems requires an extremely comprehensive and detailed audit program.

What is SecurityExpressions Audit & Compliance Server?

SecurityExpressions Audit & Compliance Server is a server with a Web-based management interface that runs on a server having Microsoft IIS and an the ASP.NET infrastructure installed. It performs audits automatically, based on network-connection status or a defined schedule. The database stores the server configuration, connection history and audit results. The Audit & Compliance Server performs three main functions:

- Self-Service Audit
- Audit-On-Schedule
- Audit-On-Connect (optional; purchased separately)

Self-Service Audit

Self-service auditing allows users to audit just their local computer. Typically a person doing self-service auditing is not the SecurityExpressions Administrator. This local system audit occurs from a designated Web page and applies the settings such as the policy files defined for Audit-On-Connect.

Audit-On-Schedule

Through Audit-On-Schedule, you manage audits by defining machine lists, notifications, and when to run tasks.

Audit-On-Connect

Audit-On-Connect, or network auditing, occurs when a device appears on the network. A system administrator or auditor would typically have these administrator privileges to Audit-On-Connect. These administrators can view or configure the network audits.

Important Concepts

Before you begin to use SecurityExpressions Audit & Compliance Server, it is important to become familiar with fundamental audit, server, and system security policy concepts and terminology.

Policy Files

Security policies lay a solid foundation for the development and implementation of secure practices within an organization. In SecurityExpressions, policy files contain the rules to which an organization must adhere for their system security configuration. Compliance with policies requires an understanding by staff of not only the individual policies but also of the circumstances in which such compliance is expected in their daily activities. Policy files have a .SIF extension.

A high-level security policy may outline specific requirements or rules that must be met. For example, a policy would cover the rules and regulations for appropriate use of the computing facilities. A technical standard or configuration guideline is typically a collection of system-specific or procedural-specific requirements that everyone must meet. For example, you might have a standard that describes how to harden a Windows NT workstation for placement on an external network (DMZ). Administrators must follow this standard exactly if they wish to install a Windows 2003 workstation on an external network segment.

The Security Policy File Library provides pre-defined and customizable system security policy files and security guidelines from well-known sources, such as Microsoft, SANS, NSA, NIST, Department of the Navy, as well as policy files including Microsoft HotFixes, user settings, and Solaris patch management. You can select a policy file to use or modify for your audits.

Policies

When you create a new Policy, you assign a name and a policy file (.SIF) to the policy. Note that Policies differ from policy files. The Policy contains the designated policy file.

From the Policies page you configure policies to use later when configuring the Profile, which defines the audits. In the Profile you associate one or more policy files with specific conditions for use in the Profile table.

User Roles

If the tasks involved in auditing computers for security compliance are divided among different people in your organization, we recommend establishing user roles to control who can use different features in this application. Several key pages contain settings that let only members of specified Windows User Groups access certain pages and their features. This allows each user to focus on their tasks while preventing unauthorized users from performing restricted operations.

You may restrict access to the pages or features themselves, plus the reports and audit results based on the restricted machine lists, policies, scopes, and scheduled tasks.

Profile

Profiles specify which policy to use for each scope. The Profile is the final specification of what to audit and how. You associate scopes with specific policies and notifications.

Scopes

Scopes are filters used to define a set of systems that get audited a specific way when using the Audit-on-Connect method. When the network detects a device, SecurityExpressions Audit & Compliance Server evaluates all scopes in order. The first scope that matches the device is the scope used. Auditing systems outside the scope does not occur.

Scope Types

The Scope Type is any of the Scopes defined in the Scope table. Scope Types include:

- IP Range
- Windows Domain
- Organizational Unit
- DNS Domain Name
- Device Type
- Machine List
- Expression

- Detection Method

Scope Value

The scope in the specified type. For example:

IP Range- A range of IP addresses or a list of IP addresses. Use **-** or **:** to indicate an IP range, such as 192.168.10.1-62.
DNS Domain Name - A domain name in DNS format that may including a wildcard, such as *.altiris.com

Notifications

When configuring the server, you can specify if you want to receive email or program-output notifications. Notifications apply to Audit-On-Schedule or Audit-On-Connect results and each audit can have one or more notification actions upon completion.

Active Policy

If the policy is Active (Yes) with a particular scope, then apply the policy. SecurityExpressions Audit & Compliance Server does not apply an inactive policy (No) but does not delete it.

Link Types

Auditing can occur on a fast or slow link, or both links. For example, it can take a long time to apply a large policy file, such as MS Fixes, over a slow link such as a 56K modem. You should configure to use this policy file only on a fast link. The SecurityExpressions Audit & Compliance Server can detect the speed of a link over which a system is audited. Certain policies may not be appropriate for slow links due to the large amount of data they request. Use the link type settings to determine if a configured Audit-On-Connect should run over slow links, fast links, or both link types.

Configuration Rule (.CONGFIGURE)

Some policy files, such as the NSA Guidelines for Windows XP and Windows 2000, contain a special rule named .CONFIGURE. The .CONFIGURE rule allows you to configure your policy files and set global parameters for policy files at run time.

Certain information is unique and distinct between systems or groups of systems. A run-time policy variable allows administrators to use a single policy file but allows identification of unique rules that require variable information. When a policy file uses a variable, your organization can use one policy file for

multiple conditions where variables differ between departments or Machine Lists. (For more info about Machine Lists, see the SecurityExpressions online Help.)

When you create a new Policy and select an associated policy file, SecurityExpressions server determines if a .CONFIGURE rule exists and displays prompts for modifications. This rule may require synchronization between the database and the policy file. To synchronize the database and the new file, save the policy file in the database with a new name with new parameters for the .CONFIGURE rule, if previously saved in the database.

Posture Condition The rules that determine whether the result of the audit is considered passing or failing. The posture condition is a final outcome of the rules' results based on whether the audit passes or fails and the impact and priority settings. The posture condition can be Always Pass, Any Fail, Any Not OK, Any Not OK with Priority, Any Not OK with Score, Any Not OK with Impact, Any Not OK with Key.

Scope Order Numeric order in which all scopes are checked for a device when it connects to the network.

Scope Name Name of the scope created on the Scope page. The named Profile associates one or more policy files to a particular scope.

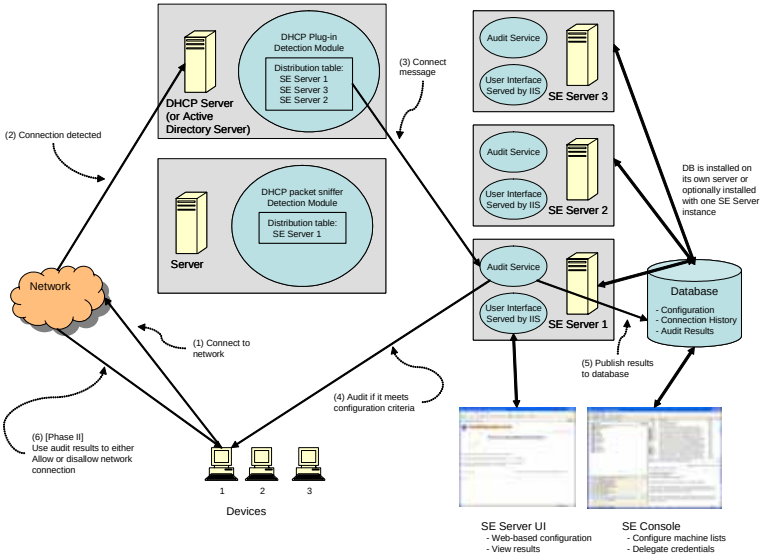
Exceptions Exceptions specify a list of devices to exclude from auditing. To exclude the devices from an audit, you must explicitly specify them in the exceptions list.

Components

The SecurityExpressions Audit and Compliance Server consists of the following components:

- Service that performs all auditing
- Database to store configuration data and audit results
- Web-based user interface to configure the auditing service

The following architecture diagram shows integration of the console, server, connection monitors, and database.



You may install multiple servers. Each SecurityExpressions Audit and Compliance Server installation includes the service for auditing and storing results and a user interface to be served through a co-resident instance of the Microsoft IIS Web server. All SecurityExpressions Audit and Compliance Servers in a single group share a single common database that stores all configuration settings, policy files and audit results for multiple servers.

SecurityExpressions Console

SecurityExpressions Console connects to a database. You can connect to the default database included with the software, or use Microsoft SQL Server or Oracle. From the SecurityExpressions

Console you can configure Machine Lists, a collection of computers specified by the system name or IP address, which you can audit as a unit. You can also delegate credentials. A Machine List might include all computers in an organization, a department, a geographic territory, domain, or the entire network. Each computer can have an optional user name and password to use as credentials for performing audits. The SecurityExpressions Console also allows you to customize policy files and use SecurityExpressions advanced reporting capabilities.

SecurityExpressions Audit & Compliance Server

An organization might deploy multiple servers where each performs audits and stores results. The server manages configurations and performs audits, and multiple servers provide for scalability and failover. SecurityExpressions Audit & Compliance Servers can be load balanced through a configurable round-robin access method used by the Connection Monitors. You can schedule audits on any one of multiple servers sharing the same database.

Database

All servers share a common database that stores configuration settings, policy files, and audit results. Storing data in a central database reduces redundant work and increases efficiency through shared information.

You can install and use the database engine included with the SecurityExpressions Audit & Compliance Server installation, Microsoft SQL Server, or Oracle. All servers and consoles using the same database comprise the same system.

Many systems and security administrators across the organization may use SecurityExpressions. Often these administrators produce similar Machine Lists and host information. Central Machine List management using the database allows this information to be stored centrally to reduce redundant work and increase efficiency through shared information.

Connection Monitors

Connection Monitors determine when a device connects to the network and then send a request to a server to perform an audit of that device. You can install them on DHCP Servers, Active Directory Servers, or other servers. Each Connection Monitor can

contain configuration files that consist of a list of audit servers to contact. This list includes a particular range of IP addresses, along with a distribution method to balance the load among the audit servers.

Console and Server Interactions

A complete security-management solution includes the server software and the console software, both using the same central database. Each offers its own unique combination of auditing and compliance features. They work best when used together but either application can be used alone if you wish.

Feature Differences

The following table shows the differences between the server and console software. The symbol ⊗ indicates when an application contains the feature.

Feature	In Server?	In Console?
Secure Web Server; Interface Accessible from Anywhere	⊗	
Separate User- and Group-Level Security for Each Feature	⊗	
Platform-Independent Interface	⊗	
Role Assignment	⊗	
Agent or Agentless Auditing	⊗	⊗
Scheduled Audits	⊗	⊗
Audit-on-Connect with Load Balancing	⊗	
Self-Service Audits - local system only; optional agreement enforcement	⊗	
Manual Audits - any number of systems at any time		⊗
Centralized Database Shared by Server and Console	⊗	⊗
Database Cleanup	⊗	

Feature	In Server?	In Console?
AuditExpress - for basic vulnerability audits		⊗
Web-services layer	⊗	
Policy Files	⊗	⊗
Ready-Made Policy Files with Update Service	⊗	⊗
Audits Against Multiple Policy Files at Once	⊗	
Customizing Policy Files and Rules		⊗
Scope-Based Dynamic Auditing	⊗	
Machine Lists	⊗	⊗
Creating Secure Personal Lists - must be logged in as the same user that created a list in order to use it	⊗	
Creating Global Lists - shared by the server and console		⊗
Creating Dynamic Lists - maintained indirectly		⊗
Reports	⊗	⊗
Results Browsing	⊗	
Credential Stores	⊗	⊗
Delegating Credentials		⊗
Notifications	⊗	⊗
Email	⊗	⊗

Feature	In Server?	In Console?
Run Command	⊗	⊗
Dump Report		⊗
SNMP		⊗
Windows Event Log		⊗
UNIX System Log		⊗
CRM Systems such as Altiris Helpdesk		⊗
Trace Routes	⊗	
Expressions Searches		⊗
History Log and Rollback		⊗
Remediation		⊗
Bandwidth Throttling	⊗	⊗

Task Workflow Between Server and Console

Each component is best suited for certain tasks. In order to take advantage of SecurityExpressions' high-level security and flexible maintenance, deploy the server software and the console software in strategic locations that can access the central database. Then use each component to perform particular tasks.

Note

To learn more about deploying the server software, turn to Chapter 2, "Before You Install," on page 19.

1 Decide whether to use the **server, console or a combination** of the two to perform scheduled audits.

You can create scheduled audit tasks to run on different servers through a single Web interface. This is ideal for large installations.

2 Decide which target systems should use an agent to connect to the software.

You have the option of auditing target systems through an agent or agentlessly. Agentless audits require credentials. Agents must be installed, plus they require Windows access groups that can access the target system.

Since each method has different credential requirements and implications on user roles, decide now which targets will be audited using an agent. Then install the agent where appropriate.

3 If you are separating tasks among different users, determine who performs the following functions.

Server functions:

- upload policies to servers
- create and edit machine lists
- create, schedule and run audit tasks
- generate reports
- configure the server(s)
- configure Audit-on-Connect

Console functions:

- create and edit policies
- enter and delegate credentials for agentless auditing

The server uses Windows authentication and groups to determine who has access to each function. Create Windows User Groups based on the access level you plan to grant different users of the server.

4 **Console:** Set up machine lists and delegate credentials.

The console allows you to delegate credentials to the server through machine lists. Once delegated to the server, the server can use them in Audit-on-Connect tasks or scheduled audit tasks.

Machine lists allow you to group target systems for different purposes. For example, a machine list might contain systems in the same department, that have the same credentials, that are owned by the same administrator, or that have an agent installed.

Systems can appear in more than one machine list.

5 **Console:** Create custom policy files.

You may use policy files exactly as they appear in the policy file library but typically organizations customize policy files to enforce their own internal policies. You may create new policy files or rules from scratch or modify copies of existing policy files and rules to meet the organization's needs.

6 **Server:** Assign roles to users.

Several key pages in the server application contain settings that let only members of specified Windows User Groups access certain pages and their features.

- Go to the Page Access page and assign the Windows user groups you created in Step 3 to each page in the server application.
- Then establish user roles for individual machine lists, policies, scopes, and scheduled tasks by entering Windows Group Access settings on the following pages:
  - Machine List Access
  - Policies
  - Scopes
  - My Machine Lists
  - Scheduled Tasks

  You may restrict access to the pages or features themselves, plus the reports and audit results based on the restricted machine lists, policies, scopes, and scheduled tasks.

7 **Server:** Create tasks for any audits you need done on a schedule.

This process involves creating policies and setting a schedule.

- Create policies, which consist of a policy file (or more, if using Audit-on-Connect) plus some other settings. When you associate a policy with a scheduled audit task, the target system(s) are audited against all policy files in the policy and according to all settings in the policy.
- If you want to use notifications, create them in the **server or console**.
- Create the scheduled audit task, assigning the appropriate machine lists, policy and notifications.

8 **Server:** Set up Audit-on-Connect for systems you need to audit whenever they connect to the network.

This process involves creating profiles, which associates policies with scopes.

- Create policies, which consist of one or more policy files plus some other settings. When you associate a policy with an Audit-on-Connect profile, the target system(s) are audited against all policy files in the policy and according to all settings in the policy.
- Create scopes, assigning the appropriate credentials to them and arranging them in the order you want them checked.
- If you want to use notifications, create them.
- Create profiles, associating policies with scopes and notifications if you're using them.
- If you want to use exceptions, create them.

9 Install and configure connection monitors to detect Audit-on-Connect activity.

Complete a configuration file (dmconfig.txt) for each connection monitor installed. Then, on the Connection

Monitors page in the server application, compile a list of all connection monitors installed and their passwords.

10 **Server or Console:** Review audit results and generate reports.

Each component offers different reports. Once audit results are in the database, you can generate reports from whichever component has the reports that suit you.

CHAPTER 2

Before You Install

Before you install SecurityExpressions Audit & Compliance Server components, you should make some decisions about your database, network devices, and SecurityExpressions servers. This chapter identifies considerations for scalability planning, database use, installation and Connection Monitor deployment.

Database Deployment

When planning your database deployment, take into consideration the following database concerns:

- Which database should I use?
- Where should I install the database?

The answers to these questions depend on your environment and scalability needs.

Which Database?

If your corporate database is one of the ODBC-compliant databases this listed in the "System Requirements" on page 31, you should consider using it to store SecurityExpressions configuration and audit results. You can connect your existing database to SecurityExpressions during the installation by identifying the Database host name and catalog (database) and the appropriate database credentials, which include the login and password. If you plan to use the corporate database, you should create the catalog (database) and its credentials before installing the SecurityExpressions Audit & Compliance Server.

If you do not have a corporate database to use, the SecurityExpressions Audit & Compliance Server installation provides an optional installation of a preconfigured default database.

Note

The default database has size limitations. Most SecurityExpressions deployments are best suited to use enterprise ODBC databases, such as Microsoft SQL Server and Oracle.

Where to Install the Database

Once you determine which database to use, you should consider where you want the database installed. It can exist on its own server or co-reside with the SecurityExpressions Audit & Compliance Server. Remember that the system, whether it consists of one or multiple SecurityExpressions Audit & Compliance Servers, interacts with one central database.

If you install the default database that came with the software, the default installation places it on same computer as the SecurityExpressions Audit & Compliance Server.

Connection Monitors

A Connection Monitor installed on the network determines when a device connects to the network and then requests a server to perform an audit of that device. Each Connection Monitor can contain a configuration file that includes a list of audit servers to contact. This list might consist of a particular range of IP addresses along with a list of SecurityExpressions servers to balance the load among the audit servers.

The SecurityExpressions Audit & Compliance Sever includes three types of Connection Monitors:

- DHCP Network Connection Monitor with access to network traffic, installed on any server, monitors network packets for those containing DHCP protocols.
- Microsoft DHCP Server Connection Monitor, installed on the device running Windows DHCP Server.
- Active Directory Connection Monitor, installed on any server on the domain, monitors Active Directory activity for when a new device appears on the network.

You must configure the sever, using the Web application, to recognize the Connection Monitors you plan to use. If the IP address or the fully-qualified name of a Connection Monitor you use does not appear in the Device Connection Monitor list, the server software won't audit any connecting target systems the monitor detects.

Distribution Process

The detection and distribution process is as follows:

1 Device connects to the network.

2 Connection Monitor detects the connection.

3 Connection Monitor sends connect message to the SecurityExpressions Audit & Compliance Sever, driven by the distribution table.

4 SecurityExpressions Audit & Compliance Sever audits devices according to the profile.

5 SecurityExpressions Audit & Compliance Sever writes results to the database and sends notifications.

Connection Monitor Configuration File

Each Connection Monitor contains a text file named dmconfig.txt that resides in the same directory as the Connection Monitor. This text file contains an IP Range and Options section and may contain a Default section.

IP Range Section

The IP range section consists of:

- IP and default IP range of the target devices
- Distribution methods
- Comma-separated list of audit server names
- Comments or description of the IP range

IP Ranges

The IP Ranges section of the configuration file identifies the IP ranges of the device groups.

- Zero or more IP ranges – IP ranges divide newly detected devices into different groups. If an IP range does not exist, no devices are audited.
- Default IP range – All IP addresses not previously placed in one of the IP range groups.

Distribution Methods

You can use one of two distribution methods for connection-monitor sequencing.

Round Robin

Each SecurityExpressions Audit & Compliance Server in the list is contacted in sequence as new devices are detected, wrapping around to the beginning of the list after contacting every listed audit server. If a connection times out, the Connection Monitor tries the next audit server in the list until it attempts contact with every audit server on the list.

First Available

To begin, the Connection Monitor always contacts the first Audit & Compliance Server in the list. If the connection fails, it tries to contact the second audit server, and so forth, until connection is

successful after trying to contact one or every audit server on the list. The First Available method is important if the first server goes down.

Comma-Separated List of Servers

Includes the names of the audit servers. A comma separates each server name.

Comments

Include any notes or explanations to clarify the audit configuration.

Options

The Options section of the configuration file contains any settings needed to control the Connection Monitors, such as enabling logging and identifying the location and name of the log file.

Port

The port you want a connection monitor to use to communicate with the server software. This entry must match the server's configuration, which is 9009.

Log Enable

Typing **True** turns logging on. Typing **False** turns logging off.

LogFile

Identifies the log file location and file name.

Password

Add the encrypted password.

DropPXE

Enables you to ignore PXE DHCP requests if using the DHCP Network Connection Monitor or Microsoft DHCP Server Connection Monitor. When the PXE gets a DHCP request, Audit-on-Connect is triggered. When PXE is done and Windows restarts, Audit-on-Connect is triggered once more, not necessarily using the same IP address.

If set to **1**, PXE DHCP packets are ignored. If set to **0**, they are processed.

Default

The Default section identifies all IP addresses not previously placed in one of the IP range groups.

IPRange

Set to default.

AuditServers

Comma-separated name of the servers.

DistributionMethod

Set to Round Robin or First Available.

Comment

Additional notes for items not explicitly specified.

Active Directory

Set the Active Directory (event log) monitoring options.

IncludeAllDomainControllers

Retrieves names of all Domain Controllers on the Domain system where the monitor resides and monitors the event logs of all Domain Controllers. One (1) is the default setting. If IncludeAllDomainControllers=0 you must add the Include key and identify the device to monitor.

Exclude

Comma-separated list of device names to omit from monitoring.

Include

Comma-separated list of device names to monitor.

Configuration File Syntax

To specify configuration data, you manually edit the dmconfig.txt file and include the required information about the IP ranges. After editing the configuration file, you must stop and restart the service through the Service Management Console, which is accessible through Administrative Tools.

Important

Be aware that if you're using the DHCP Plug-In Connection Monitor, its Microsoft's DHCP Server Service that you have to

stop. Since this service controls other functions on the network, stopping it might have other temporary effects on the network.

Note

Use the # character at the beginning of all comment lines to ensure they get ignored when the file processes.

The configuration data syntax is similar to .ini file syntax, such as:

```
[IP_RANGE_1]
IPRange=10.0.3.0:254
AuditServers=server1,server2
DistributionMethod=Round Robin
Comment=Home office ip addresses

[IP_RANGE_2]
IPRange=10.0.2.0:254
AuditServers=server3,server1,server2
DistributionMethod=First Available
Comment=California office ip's

[Default]
IPRange=Default
AuditServers=server1,server2
DistributionMethod=Round Robin
Comment=Catch anything not explicitly specified

[Options]
Port = 9009
Password = AES:cb789817f8d99c7e5a1e5beb8510bf71
LogEnable=True
LogFile=c:\temp\dhcpdetect.log


[ActiveDirectory]
IncludeAllDomainControllers=1
Exclude=server1, server2
Include=server3
```

Processing the Configuration File

When the Connection Monitor recognizes a new device on the network, it compares the device IP address to the IP ranges defined in the configuration file, excluding the Default settings, starting with the first range in the file and proceeding in order. If the address falls in one of the IP ranges, that group's audit server list and distribution method determine where to connect.

If the IP address does not fall within any of the specified ranges, a group whose IPRange=Default accesses the audit server list and distribution method.

You do not have to specify a Default IP range. However, if a Default range does not exist and the IP address does not correspond to any of the defined ranges, no connection monitors contact the audit server and the device remains unaudited.

CHAPTER 3

Installing and Configuring the Audit & Compliance Server

These instructions guide you through the server installation on your Windows systems. Before you install SecurityExpressions Audit & Compliance Server, it is important to understand its overall operation, the interaction of the components, and the interaction with SecurityExpressions Console. You must have a thorough understanding of the system scalability and operation in their environment before installing.

Installation Overview

Download SecurityExpressions Audit & Compliance Server from www.altiris.com.

If you will be using Audit-On-Connect, you must install Connection Monitors on DHCP servers or Active Directory servers throughout the enterprise. Connection Monitors are installed separately.

Note

If you plan to use Audit-on-Connect, you must purchase a separate license for it.

System Requirements

Install the server software on any system that meets the following minimum requirements.

Hardware

- 512 MB RAM minimum
- 500 MB of free disk space

Software

One of the following operating systems:

- Windows 2000 Server
- Windows 2003 Server

Additional software:

- Microsoft Internet Information Services (IIS) 5.0 or later

Optional ODBC Databases

- Microsoft SQL Server 2000 or 2005
- Oracle 8, 9, or 10

Connection Monitor

- Install on a connection-monitor server running Microsoft Windows 2000 or later

Note

To access the server application remotely, you can use any system **on any platform** running Internet Explorer 5.0 or later.

Server Installation

You may wish to install multiple instances of the SecurityExpressions Audit & Compliance Server, one per system. During the installation, you install a default database or connect to an existing database. If you choose to install a default database, a preconfigured database is installed co-resident with the server.

For example, a common installation scenario includes installing the default database with the first server installation and then during subsequent server installations, identifying the database installed with the first server as the central database. Alternately, if your organization already has an ODBC database, the server can connect to that database.

Upgrading Notes

If you are upgrading from a previous version of the software, then you might already have a central database that contains audit and compliance data. Back up the database before installing either the server or the console software. The process of upgrading the console software upgrades the database schema. After the upgrade, the database will no longer work with older versions of the console or server software.

The console software has the option of using table prefixes to connect to the database, while the server software cannot use table prefixes. Make sure the database you plan to use does not require a table prefix in order to connect to it. If you are upgrading an older database and you created the database with a table prefix, you must connect the server software to it with a user account that can access the database directly without the need for a table prefix. Examples:

- **SQL Server -** this could be a user with a db_owner role for the database.
- **Oracle -** this could be the schema owner.

Consult your database documentation for other possible users.

Server Installation Procedure

To install SecurityExpressions Audit & Compliance Server, run Setup.exe and complete the Wizard.

1. View the **Welcome** page.
2. On the License Agreement page, select **I Agree** to accept the terms of the license. You cannot continue with the installation until you accept the agreement.
3. On the **Default Database** page, select **Yes** to install a **Default Database**. Select **No** if you plan to use an existing database.

   If you choose **No**, you connect to the database when you run SecurityExpressions Audit & Compliance Server.

   If you choose **Yes**, set the password for the database's Administrator account.
4. **Select Installation Address** by providing the name of a virtual directory and a **Port** number.

   We recommend using the default port and installation address.
5. When you **Confirm Installation**, the installation begins. A message appears when the installation completes and reminds you to keep current with the .NET updates.

Removing SecurityExpressions Audit & Compliance Server

You can remove SecurityExpressions Audit & Compliance Server by one of two methods:

1. In **Control Panel**, double-click the **Add/Remove Programs** icon and select SecurityExpressions Audit & Compliance Server.
2. Run the Setup Wizard. Select to either Remove or Repair. Remove takes the software off the computer and offers a chance to stop the process before proceeding.

Configuring IIS

After installing the software, you might need to configure Internet Information Services (IIS) for use with the software. Depending on your auditing environment, you might not have to do anything and can proceed to "Getting Started with SecurityExpressions Audit & Compliance Server" on page 42. Review the following sections about special IIS-configuration procedures. Perform any procedures that apply to you before opening the application for the first time.

Server Certificates for Windows 2000 Users

If you installed the server software on Windows 2000 Server, you need to assign a server certificate to the Web server to ensure secure access using HTTPS.

Note

Skip this procedure if:

- you installed the server software on Windows 2003 Server. The server certificate was automatically assigned for you.
- you already have a server certificate assigned to this Web server. The SecurityExpressions Audit & Compliance Server Certificate is provided as a convenience in case The Web server does not already have a server certificate assigned to it.

To assign the SecurityExpressions Audit & Compliance Server Certificate:

1. Go to **Start > Administrative Tools > Internet Information Services (IIS) Manager**.
2. In the left pane's tree, navigate to \Local Computer\Default Web Site\.
3. Right click the \Default Web Site\ folder and select **Properties** from the right-click menu that appears.
4. In the Properties dialog box, click the **Directory Security** tab to make it active.
5. In the Secure Communications box, click the **Server Certificate** button. The Web Server Certificate Wizard appears.
6. Click **Next** to start the wizard.

7 In the Server Certificate page, select **Assign an Existing Certificate** and then click **Next**.

8 Highlight **SecurityExpressions Audit & Compliance Server Certificate** in the Available Certificates list and then click **Next**.

9 The Certificate Summary page appears. Click **Next** to install the certificate.

10 Click **Finish** to close the wizard.

Authentication Access Methods

When you install the server software, the Integrated Windows Authentication option in Internet Information Services Manager becomes enabled for the \seserver\ application folder. This is the integrated Windows authentication access method you must use.

Configuring the Port Number for SQL Server Users

If you're using Microsoft SQL Server as your database software and are not using the standard port number (1433) to connect to it, you need to make the Audit and Compliance Server aware of the correct port number. You can do this in the Windows Registry.

To configure a nonstandard port number for use with the Audit and Compliance Server:

1 Open the Windows Registry Editor.

2 Go to HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\MSSQLServer\Client\ConnectTo and add the following REG_SZ value:
servername1 REG_SZ *connectiontype,servername2,port#*
where:

servername1 is the name or IP address of the computer running SQL Server

connectiontype is the network-connection type, such as dbmssocn for Winsock TCP/IP

servername2 is the same string as *servername1* (no interchanging IP addresses and computer names in the same value)

port# is the nonstandard port number you're using

3 Close Registry Editor.

Installing Connection Monitors

If you purchased a license for the server software's Audit-on-Connect feature, you'll need to install connection monitors on DHCP Servers, Active Directory Servers, or other servers that coordinate Audit-on-Connect sequences.

To install a connection monitor:

1. Copy the \ConnectionMonitors\ folder from the Zip installation package to the server coordinating Audit-on-Connect sequences.
2. Launch **Setup.exe** in the folder.
3. When the setup wizard appears, click **Next** to begin the installation.
4. In the License Agreement page, select **I Agree** and click Next.
5. In the Choose Connection Monitors page, select the connection monitor(s) you want to install on this server. Then click **Next**.
6. If you selected **Active Directory Monitor** in step 5, the Active Directory Monitor User page appears. Type the user name and the password of the user you want the service to run as.

Important

If you didn't select **Active Directory Monitor** in step 5, the Active Directory Monitor User page does not appear. Skip this step.

Type the user name in the form **domainname\username** if the account a network-domain account, or **.\username** if the account a local-machine account.

Before proceeding, make sure this user has the rights "Manage auditing and security log" and "Log on as a service." To check user rights, select Local Security Policies from Administrative Tools and browse to Security Settings\Local Policies\User Right Assignments.

7 In the Select Installation Folder page, browse to a new installation path if necessary. Then click **Next**.

8 Click **Next** again to confirm that you want to install the connection monitor(s) now.

9 A status bar shows the progress of the installation. When the installation is complete, click **Close** to exit the setup wizard.

Now you may configure the connection monitor whenever you're ready. For instructions, open the server application, go to the Connection Monitors page and click the **?** help icon at the top of the page.

Removing Connection Monitors

You can remove connection monitors using one of these methods:

- In **Control Panel**, double- click the **Add/Remove Programs** icon and select SecurityExpressions Audit & Compliance Server.
- Run Setup.exe again.

Either method removes SecurityExpressions Audit & Compliance Server.

1 The Remove wizard opens a Welcome page that explains that the software will be removed.

2 Select either **Remove** or **Repair** to either remove the software. Both options provide a chance to cancel before proceeding.

3 Removing shows the status of the software being removed.

4 Finished declares that the remove or repair installation completed.

This page shows the status of the software being removed. In the case of the DHCP Server Callout API dll, the DHCP Server probably needs to be stopped before the file is deleted, and then restarted afterwards.

Installing the Altiris Agent

If you have Altiris® Notification Server™ software, the server application gives you the ability to send audit notifications to Notification Server as Notification Server events. In order to take advantage of this feature, you must install the Altiris Agent on the computer running the server application. You can accomplish this through the Altiris Console's Solution Center by pushing the Altiris Agent to the computer running the server application.

Tip

To learn more about the Altiris Agent, Altiris Console, or Notification Server, you can download the documentation for these and any other Altiris product from www.altiris.com/Support/Documentation.

Getting Started with SecurityExpressions Audit & Compliance Server

To access the server application securely, do one of the following:

- click the **SecurityExpressions Server** shortcut placed on the desktop when you installed the software.
- open a Web browser and go to https://*servername*/seserver, where *servername* is the name of the Web server.

If opening the application for the first time, the Application Setup page appears. Before you can continue, you must:

1 connect to the database

2 create a credential store user

3 register the software

Connecting to the Database

The Application Setup page is where you connect to the database. If you plan to install the server software on more than one system, they should all connect to one central database. The central database can either be the default database that you can install when you're installing the software or one of the supported enterprise ODBC-compliant databases.

The database settings provide the connection information for the SecurityExpressions Audit & Compliance Server database. All servers connecting to the same database are part of the same SecurityExpressions Audit & Compliance Server system.

Important

If you installed the default database when you installed this copy of the server software, you are already connected to the database. Skip this procedure.

To establish a valid database connection:

1 In Database Type, select the manufacturer of the database you plan to use from the drop-down list. If you installed the default database when you installed the software, select **Firebird**.

2 In the Database Server Name box, type the name of the system containing the central database you want the server software to use.

   If you installed the default database along with the server software, the Database Server Name box automatically contains the name of the local system. Don't forget to change the name if not using this as the central database.

3 In the Catalog (Database) Name box, type the name of the database you want the server software to use.

   If you installed the default database along with the server software, the Catalog (Database) Name box automatically contains the default database's default name. Don't forget to change the name if not using this as the central database.

4 Type the database user name and password to log in to the database.

5 Click **Apply** to complete the connection.

Now this installation of the server software is connected to the central database. Make sure to connect all server applications you install in the organization to this database.

Creating a Credential Store User

Before you can use the software to audit systems, you must have a valid database connection and a server credential store. The credential store holds all credentials to be stored in the database.

When an audit begins, it obtains the credentials of the newly connected computer from the audit server’s configured Credential Store. If it does not find these credentials, it looks for the delegated credentials.

You must specify a Credential Store to use SecurityExpressions Audit & Compliance Server. Choose the Credential Store, type the Credential Store password, and click **Apply**.

On the SecurityExpressions Audit & Compliance Server, you can create new Credential Stores on the Setup page, adding them to the database, but you cannot modify them. Or, you can use Credential Stores previously created from the SecurityExpressions Console.

Important

Each collection of servers must use the same Credential Store.

Registering the Software

You must enter a valid license key in order to activate the server application. If you purchased the Audit-on-Connect component, you must activate that feature with a second license key.

To add or change the current license, enter a license key and click **Apply** to register it. If the license key is invalid, a warning appears.

Where to Go from Here

Once you complete the installation of all components, begin configuring the server to perform an audit.

Index

U

W